Data Protection Officer Role:

(Risk rating key can be found at the end of the document)

GDPR Reference	Data Protection Officer/Organisation Responsibilities	Meeting of Responsibility	Action Required	Risk Rating (RAG or B=No current risk)
Position of the DPO				
Article 37 (5)	The data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 39.	• The DPO is not an expert in this area but does have an increased understanding of legislation compared to other staff • Not a full-time role so will not be an expert in this area. Also proves difficult to learn on the job as not immersed in the topic frequently enough. • Can be a large complex area which requires reading time to support decision making which isn't available due to other responsibilities • Training courses attended where needed • Support can be provided by the Joint GWP/SWP DPO but they are extremely busy and the resource can not be relied upon although they do assist if able.	• Continuation of training where able • Consideration to putting in place external support, possibly on an all Wales basis, to be accessed when required. This can be picked up in the external audit being undertaken in 2021/22. • Assess whether any additional support can be provided to the other responsibilities within the HoAC role to allow time to develop data protection knowledge. If not possible, the role of the DPO may need to be re-considered with possible options developed further including sharing a DPO with other OPCCs, appointing an external DPO or appointing an additional member of staff.	Ongoing. Work of consultant will determine next steps. Risk = Medium
Article 38 (3)	The controller shall ensure that the DPO does not receive any instructions regarding the exercise of their tasks	• CEx supportive of the work undertaken by the DPO but does not guide or set specific tasks	• Ensure this is maintained. DPO to raise any concerns if they arise.	No current risk
Article 38 (3)	The controller shall ensure that the DPO is not dismissed or penalised by the controller for performing their tasks.	• Executive team are aware • Not currently clarified in job description	• Consideration given as to including clarity in job description	Ongoing but on target. Risk = Low
Article 38 (3)	The controller shall ensure that the DPO reports directly to the highest management level of the controller	• HoAC is the DPO and attends the OPCC Management Board • Regular meetings with the CEx (every 2 months) to discuss data protection action plan • First annual report developed and will be reported to OPCC Management Board • Brief overview of data protection work/compliance provided at every OPCC Management Board	• Finalisation of annual report for 2020/21. Once report template is in place reporting in future years will be made easier.	Ongoing but on target. Risk = Low
Article 38 (1)	The data controller must ensure that the DPO is involved, properly and in a timely manner, in all issues relating to the protection of personal data;	• Reliance is on staff to inform the DPO of any relevant projects that would contain personal data. DPO has provided advice on projects. • Not many projects exist within the OPCC that involve information such as this • Attendance at OPCC Management Board where all projects should be discussed	• No specific action needed, • Annual refresher training will act as a reminder to staff • Consideration of data protection issues has also been built into the project initiation documentation	No current risk

Article 38 (2)	The controller shall support the data protection officer in performing the tasks referred to in Article 39 by providing resources necessary to carry out those tasks and access to personal data and processing operations (resources should include sufficient time, financial, infrastructure and staff as appropriate to enable the DPO to meet their GDPR obligations)	• Support built into Governance Officer role but unable to be provided due to time required for other responsibilities • This has impacted on the DPO's ability to undertake the role adequately and provides a risk to compliance. • The CEx has agreed for a data protection accountability audit to be undertaken by an external consultant to clarify where we are regarding GDPR compliance, what is outstanding and an action plan to maintain future compliance.	• Initial contact has been made with a consultant for a quote to undertake an audit. Will then ensure appropriate procurement process is followed prior to appointing.	On-going but risk relating to ensuring there is significant resource to support the DPO Risk = High
Article 38 (2)	The controller shall support the DPO to maintain their expert knowledge	• Support provided to DPO to attend any training courses deemed necessary • Difficulty to find time to attend training due to current workload • DPO role isn't full time so difficult to learn 'on the job'.	• Continuation of training where able • Assess whether any additional support can be provided to the other responsibilities within the HoAC role to allow time to develop data protection knowledge. If not possible, the role of the DPO/HoAC roles may need to be re-considered.	Ongoing. Work of consultant will determine next steps. Risk = Medium
Article 38 (6)	The controller shall ensure that any additional tasks and duties placed on a DPO do not result in a conflict of interest with their DPO duties.	• As the HoAC is also the DPO and the Deputy Monitoring Officer (DMO) we have had to ensure no conflict of duties exists • ICO confirmed they did not believe there was a conflict between the roles of DPO and DMO • HoAC would normally have held decision making responsibilities in relation to processing in data protection policies, these have had to be allocated to the CEX to remove the conflict of interest that arises	• Continue to monitor whether changes to current HoAC role cause a conflict of interest with the role of the DPO • Request external consultant to review to provide assurance there aren't any conflicts currently in existence. To take place in 2021/22	Ongoing but on target. Risk = Low
ICO – DPO's	The controller gives the DPO appropriate access to other services within the organisation so that they can receive essential support, input or information	• DPO is able to contact other departments as needed who have supported work in their areas. • Direct access to the CEx ensures any issues can be raised as needed.	• Workloads of other departments can impact on the support provided but not currently an issue. • Will continue to monitor and raise any concerns.	No current risk
Tasks of the DPO				
Article 39 (1)(a)	The DPO will inform and advise the organisation and its employees about the obligations to comply with the GDPR and other data protection laws;	• DPO provides advice when requested • Majority of organisational policies sit with the HoAC so data protection is considered in their development • DPO attends meetings where any policy should be presented for comment/approval • Monthly data protection update provided to OPCC Management Board	• Need to ensure maintain awareness of changes to data protection law, case law and best practice. This is currently difficult due to the other responsibilities placed on the DPO in their role as HoAC.	Ongoing but limited time to ensure compliant with emerging DP issues/best practice could be problematic in the future. Risk = Medium

Article 39 (1)(b)	The DPO is tasked with monitoring compliance with the GDPR and other data protection laws, OPCC data protection policies, awareness-raising, training and undertaking and commissioning audits;	• Not currently monitoring compliance and there are a couple of large pieces of work outstanding on original GDPR action plan • An internal audit was undertaken in July 2018 with a follow up undertaken in January 2019 with 'reasonable' assurance achieved. No audits have been undertaken or commissioned since although an accountability audit will take place during 2021/22. • Key data protection policies (eg SARs/DPIA guidance etc) are in place but overarching data protection policy needs to be drafted • Review of SARs has not been able to take place due to resourcing issues • Difficult to maintain up-to-date knowledge of case law, changes, best practice due to other responsibilities	• Commencement of accountability audit will provide next steps to ensure this element of the DPO role can be fulfilled with a plan developed to continue to work towards compliance and for future auditing plan to be established.	Ongoing. Not currently compliant so DPO has not undertaken any auditing. Risk = Medium
	The organisation will take account of the DPOs advice and the information the DPO provides on data protection obligations;	• Advice provided as requested or if DPO identifies a need	• This is an area that will continue to be monitored and concerns raised with the CEx if necessary. • No instance of advice provided not being taken.	No current risk
	The DPO shall ensure that the organisation documents the reason why any advice given by the DPO is not followed.	• Record kept by DPO of all times advice was requested. A log will be made if the organisation chooses not to follow any advice provided.	• This is an area that will continue to be monitored and concerns raised with the CEx if necessary. • No instance of advice provided not being taken.	No current risk
Article 39 (1)(c)	The advice and input of the DPO will be sought when a Data Protection Impact Assessment (DPIA) is undertaken;	• Advice is sought when a DPIA is drafted although projects the OPCC is involved in that contain personal information are minimal. • Guidance notes are available to support OPCC staff to complete a DPIA	• This is an area that will continue to be monitored. • If the use of DPIAs becomes more prevalent specific training on their requirements and completion can be considered • Build in review of DPIA guidance into Policy Review table. • Review DPIA guidance to ensure it's up to date.	Ongoing. Risk = Low
Article 39 (1)(c)	The DPO will also monitor the performance of the DPIA pursuant to article 35 (DPIA's)	• Minimal DPIAs are in place for the OPCC but DPO has not monitored their performance to date.	• Resourcing will be considered during/post the accountability audit • Plan needed to periodically build in reviews of DPIAs	Ongoing Risk = Low
Article 39 (1)(d) & (e)	The DPO acts as a contact point for the ICO, and as such will co-operate with the ICO including during prior consultations under Article 36 (Prior Consultation) and will consult, where appropriate, on any other matter.	• ICO have name and contact details of the DPO • Any relevant contact will be dealt with by the DPO as appropriate	• No further action required	No current risk

Article 39 (2)	The DPO has due regard to the risk associated with processing operations, and takes into account the nature, scope, context and purpose of the processing;	• DPO should be consulted on the risks associated with high risk processing activities relating to personal data although these are minimal • Any data protection risks will be owned by the DPO	• Accountability audit will determine if any further work needs to be undertaken to ensure this element of the DPO role is met.	No current risk
Accessibility of the DPO				
Article 37 (7)	The controller or the processor shall publish the contact details of the data protection officer and communicate them to the supervisory authority.	• Name and contact details for the DPO are published on the OPCC website and included in all privacy notices. This information has also been provided to the ICO.	• No further action required	No current risk
Article 38 (4)	Data subjects may contact the data protection officer with regard to all issues related to processing of their personal data and to the exercise of their rights under this Regulation.	• The DPO will be available to all data subjects during the working day. • Any contact required outside of the working day can be submitted via email	• Consideration needs to be given as to the process to be implemented in the absence of the DPO for reasons such as illness or annual leave	Ongoing Risk = Low

Risk Rating Key:

BBRAG Key	
	Complete
	On hold
	Not on target - immediate/significant cause for concern
	Mainly on target - there are some minor issues that may impact completion of objective
	On target